



Manual de instalación, configuración e integración STORK para Proveedores de Servicio para .NET

Resumen: Esta es un manual para la instalación, configuración e integración a la plataforma STORK para proveedores de servicio. También integradores de sistemas se pueden beneficiar de este manual. Este manual debe ser leído por administradores e integradores responsables de integrar STORK en una aplicación en tecnología .NET.



Historial del documento

Version	*Date*	*Modification reason*
1.0	1/02/2012	Versión inicial

Índice



Lista de abreviaturas

<Abreviatura>	<Explicación>
STORK	Secure idenTity acrOss boRders linKed
PEPS	Pan European Proxy Server
SP	Service Provider (Proveedor de Servicio)
VS 2010 EE	Visual Studio 2010 Express Edition



Resumen ejecutivo

Este documento ofrece información detallada sobre como configurar, crear y desplegar en .NET una aplicación para un Proveedor de Servicios (SP) para su uso en la red STORK.

Como es necesaria la existencia de un IIS 6 para desplegar la aplicación SP, el documento comienza dando una información básica sobre el servidor.

Después de eso, se describe qué necesita saber el usuario sobre las posibles configuraciones para su proyecto.

Tras leer este manual, el administrador o integrador debería ser capaz de configurar, crear y desplegar una aplicación que sea capaz de conectarse a la red STORK.

1 Introducción

Este documento está dividido en varios capítulos con el fin de permitir al lector acceder fácilmente a las secciones más relevantes para el escenario específico en el que esté trabajando.

Primero, se aborda la configuración del servidor II6 (preparándolo para el despliegue de la aplicación SP) y se explica cómo instalar los certificados necesarios.

A continuación, en otro punto se describe cómo poner en marcha la aplicación en unos pocos minutos.

Después de eso se entra en más detalle en las posibles configuraciones, para que el lector comprenda las posibilidades que le ofrece el sistema y modifique la configuración básica adaptándola a sus propias posibilidades.

Para terminar, en la sección de Preguntas Frecuentes (FAQ) se responden algunas de las dudas más comunes.

2 Antes de empezar

Asegúrese de que dispone de un Servidor Windows con IIS 6 (se utilizó un Windows Server 2003 para el desarrollo de la aplicación SP) instalado con.NET Framework 4, ya que la aplicación fue desarrollada con Visual Studio Project. También necesitará VS 2010 EE (la Express Edition es suficiente) y también .NET Framework 4 instalado en su máquina local (para modificar y crear el paquete SP).

En la siguiente sección de dan las instrucciones para configurar el certifucado que utilizará el motor SAML Engine para firmar los token antes de desplegar el proyecto en IIS 6.

Con el objeto de facilitar la lectura del documento se utilizará la siguiente variable:

`$SP_PACKAGE_DIRECTORY – El directorio base con el ZIP con el contenido del paquete SP.`

2.1 Keystore

La aplicación SP usa el Windows Certstore / keystore y, por tanto, el certificado con el que firmar el SAML y el certificado del PEPS español con el que conectar debe estar instalado en él.

2.1.1 Instalando los Certificados

Para instalar el certificado para firmar el SAML y el certificado del PEPS, necesita seguir los siguientes pasos:

1. Pulse el menu "`Start`", después pulse "`run`";
2. Abra la consola Windows Certificate Management ejecutando el comando "mmc";
3. Presione CRTL + M y pulse "`Add`";
4. Seleccione "`Certificates`" y pulse "`Add`";
5. Pulse en el checkbox "`Computer account`", luego pulse "`Next`" y finalmente (cheque la opción "`Local computer`") pulse "`Finish`";
6. Cierre la ventana "`Add Standalone Snap-in`";
7. En la ventana "`Add/Remove Snap-in`" pulse "`OK`";
8. Expanda el directorio "`Personal`" en el menú "`Certificates (Local Computer)`";
9. Pulse el botón derecho en la carpeta "`Certificates`", seleccione "`All tasks`" y entonces pulse en la opción "`import…`";
10. Siga el wizard para instalar el certificado de la aplicación SP (certificado P12 ó PFX);
11. Expanda la carpeta "`Personal`" en el menú "`Certificates (Local Computer)`" y escriba en la columna "`Issue To`" el valor del certificado SAML (será necesario más adelante);
12. Expanda la carpeta "`Trusted Root Certification Authorities`" en el menu "`Certificates - CURRENT USER`";

13. Pulse el botón derecho sobre la carpeta "`Certificates`", seleccione "`All tasks`" y entonces pulse la opción "`import…`";
14. Siga el wizard para instalar el certificado de la aplicación SP (certificado P12 ó PFX).

Si no obtiene ningún error, acaba de instalar el certificado para el motor SAML Engine y el certificado del PEPS.
Ahora es el momento de cambiar los permisos del Windows Certstore:

1. Instale Windows Server 2003 Resources kit tools (puede descargarlo en http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd);
2. Abra una ventana de comandos (`cmd.exe`);
3. Vaya a `C:\Program Files\Windows Resource Kits\Tools` (directorio por defecto);
4. Ejecute el siguiente comando:

```
winhttpcertcfg -g -c "LOCAL_MACHINE\My" -s SubjectStr -a "NETWORK SERVICE"
```

5. Replace "`SubjectStr`" por el valor que le dió en la última subsección.

2.2 Configuración del Servidor

2.2.1 ISS6

Antes de desplegar la aplicación SP, necesita crear un directorio virtual en II6:

1. Abra el explorador de windows y luego la carpeta "`C:\Inetpub\wwwroot\`";
2. Cree un directorio "`SP`";
3. En "`Administrative tools`", abra "`Internet Information Services (IIS) Manager`";
4. Botón derecho sobre "`Default Web Site`", selecione "`New`" y entonces pulse "`Virtual Directory...`";
5. Pulse "`Next`" para continuar;
6. Inserte "`SP`" como alias y pulse "`Next`";
7. Pulse en el botón "`Browse`", seleccione el directorio "`C:\Inetpub\wwwroot\SP\`" y entonces pulse "`Next`";
8. Chequee las opciones "`Read`", "`Run scripts`", "`Execute`" y "`Browse`" y entonces pulse "`Next`";
9. Pulse "`Finish`" para crear el directorio virtual SP.

3 Inicio Rápido

Este inicio rápido le permitirá configurar, compilar y ejecutar el proyecto en pocos minutos, pero antes de empezar necesita configurar su servidor tal y como se describe en el capítulo anterior (vea "Antes de empezar"). Una información más detallada sobre ficheros de configuración y atributos la tiene disponible en el siguiente capítulo.

3.1 Abra Visual Studio Project

La aplicación SP ha sido creada en Visual Studio 2010 Express Edition y, por tanto, necesita tenerla instalada (además de.NET Framework v4).

Una vez que haya instalado VS 2010 EE, necesita importar el proyecto:

1. Abra VS 2010 EE;
2. Pulse el menu "`File`", luego pulse "`Open Project`";
3. Abra el directorio `$SP_PACKAGE_DIRECTORY\EN\toolkit\DemoSP.NET`;
4. Seleccione el fichero "`DemoSP.NET.sln`";
5. (El proyecto será abierto por VS 2010 EE).

3.2 Configuraciones

En VS2010 EE, sobre el proyecto DemoSP.NET, edite el fichero `web.config y modifique las siguientes propiedades`:

- **SPReturnURL** =http(s):// **insert.your.ip.here** /SP/HandleResponse.aspx
- **LOCAL.SPEPSURL** =http(s)://**insert.your.country.access url.to.STORK**

Ha concluido la configuración del SP y está preparado para ponerlo en marcha en su propia dirección IP.

3.3 Compilación y Despliegue rápido

3.3.1 Despliegue IIS6

Debe generar el paquete sobre VS 2010 EE antes de desplegarlo sobre el servidor ISS6:

1. Abra VS 2010 EE;
2. En "`Solution explorer`", botón derecho sobre el proyecto "`Common`" y pulse "`Build`";
3. En "`Solution explorer`", botón derecho sobre el proyecto "`Common.SAML`" y pulse "`Build`";
4. En "`Solution explorer`", botón derecho sobre el proyecto "`DemoSP.NET`" y pulse "`Build Deployment Package`";
5. Copie el contenido del directorio "`$SP_PACKAGE_DIRECTORY\EN\toolkit\DemoSP.NET \DemoSP.NET\obj\Release\Package\PackageTmp`" al directorio de servidor IIS "`C:\Inetpub\wwwroot\SP\`".

Por ultimo, abra su navegador y vaya a la siguiente página: “http(s):// **insert.your.ip.here** /SP/”



4 Instalando DemoSP.NET

4.1 Ficheros de configuration

El proyecto DemoSP.NET viene con una configuración que puede resultar insuficiente. En esta sección se explica cada propiedad.

4.1.1 web.config

El fichero `web.config` prove las principales configuraciones para el SP.

Key	**Description**
`SPProviderName`	Nombre del Proveedor de Servicio
`SPCountry`	País del Proveedor de Servicio (SP)
`SPQAALevel`	Nivel QAA del SP
`SPReturnURL`	URL usada cuando el Servicio Nacional STORK finaliza el proceso (es la dirección de respuesta)
`LOCAL.SPEPSURL`	Es la URL de Servicio Nacional STORK (dirección a la que enviar la solicitud)
`SPSector`	Sector del SP
`SPApplication`	Aplicación del SP
`SPVCFile`	Path del fichero de control de versiones (generado por Version Control).

Nota que hay 2 configuraciones más, que deberían tomar como valor el nombre del proveedor de servicios.

Atributos disponibles para el SP:

Key	**Description**
AttributeList	La lista de atributos separados con punto y coma
AttributeName.NS	El namespace del AttributeName
AttributeSeparator	El separador de la lista de atributos

SPEPS disponibles para enviar peticiones SP:

Key	**Description**
`SPEPS.CountryList`	La lista de países SPEPS separadas por punto y coma
`Country.SPEPSURL`	La URL del SPEPS
`CountrySeparator`	El separador de la lista de países

CPEPS disponibles para enviar peticiones SP:

Key	**Description**
`CPEPS.CountryList`	La lista de países CPEPS separadas por punto y coma
`Country.SPEPSURL`	La URL del CPEPS

Configuraciones del SAML Engine:

Key	**Description**
`SamlCertificate`	La huella digital (**no el serial number!**) del certificado a obtener del keystore de la máquina local (sin los separadores);
`SamlValidTimeframe`	Número de minutos de validez para el token
`NSQAALevel`	El namespace del atributo SAML's QAA Level
`NSQAALevelPrefix`	El prefijo del nivel SAML's QAA
`NSReqAttrs`	El namespace de atributos para las SAML Requests
`NSReqAttrsPrefix`	El prefijo de atributos para las SAML Requests
`NSReqAttr`	El namespace de atributos para las SAML Requests
`NSReqAttrPrefix`	El prefijo de atributos para las SAML Requests



5 Configurar la DemoSP.NET

En este capítulo se describe configuraciones avanzadas de la DemoSP.NET, por ejemplo como añadir nuevos países, más atributos, etc.

5.1 Atributos

5.1.1 Añadir un nuevo atributo

Si necesita añadir un nuevo atributo, debe:

1. Editar el fichero “`C:\Inetpub\wwwroot\SP\web.config`“;
2. Añadir el nombre del nuevo atributo a la “`AttributeList`” configurada (después de insertar punto y coma);

   Por ejemplo si necesita añadir el atributo fiscalNumber::

   ```
   <add  key="AttributeList"
         value="CURRENT_ATTR_LIST;fiscalNumber"/>
   ```
3. Añadir un nuevo nombre en los *namespace*:

   Por ejemplo: Añadir la siguiente línea al fichero web.config:

   ```
   <add  key="fiscalNumber.NS"
         value="http://www.stork.gov.eu/1.0/fiscalNumber"/>
   ```

5.1.2 Modificar un atributo

Si necesita modificar un nombre de un atributo, debe:

1. Editar el fichero “`C:\Inetpub\wwwroot\SP\web.config`“;
2. Modificar el nombre del atributo en la lista “`AttributeList`” configurada;

   Por ejemplo si neecsitas modificar el atributo “surname” (apellidos) a inheritedFamilyName (apellidos originales), habría que cambiar:

   ```
   <add key="AttributeList" value="CURRENT_ATTR_LIST;surname"/>
      Por
   <add key="AttributeList"
      value="CURRENT_ATTR_LIST;inheritedFamilyName"/>
   ```
3. Modificar el *namespace* del atributo:

   ```
   Cambiar
   <add  key="surname.NS"
         value="http://www.stork.gov.eu/1.0/surname"/>
   Por
   <add  key="inheritedFamilyName.NS"
         value="http://www.stork.gov.eu/1.0/inheritedFamilyName"/>
   ```



5.2 Añadir un país que da servicio a proveedores de servicio

Si necesita configurar un nuevo PEPS en la DemoSP.NET, tiene que:

1. Editar el fichero `C:\Inetpub\wwwroot\SP\web.config`";
2. Añadir el nuevo código ISO 3166 - alpha 2 del país a la configuración "`SPEPS.CountryList`" (insertando un punto y coma antes);

   Ej. Si necesita añadir a España:

   ```
   <add key="SPEPS.CountryList" value="CURRENT_COUNTRY_LIST;ES"/>
   ```
3. Añada un nuevo identificador de país.

   Ej.: Añada la siguiente configuración al fichero `web.config`:

   ```
   <add key="ES.SPEPSURL"
   value="https://88.84.94.24/PEPS/ServiceProvider"/>
   ```
4. Pedir a este país que acepte peticiones suyas, que por lo menos incluye el envío del certificado de firma del proveedor de servicio al país destino.

5.3 Añadir un país del cual aceptamos credenciales

Si necesita configurar un nuevo país proveedor de credenciales en la DemoSP.NET, tiene que:

1. Editar el fichero "`C:\Inetpub\wwwroot\SP\web.config`";
2. Añadir el nuevo código de país (ISO 3166- alpha 2) a la configuración "`CPEPS.CountryList`" (insertando un punto y coma antes);

   Ej. Si necesita añadir España:

   ```
   <add key="CPEPS.CountryList" value="CURRENT_COUNTRY_LIST;ES"/>
   ```

5.4 Iniciar la aplicación

Abra su navegador y vaya a http(s)://your.ip.addres/SP/ (si su servidor está escuchando en otro puerto cambia a URL consecuentemente). Debería ver una página similar a la Figura 1.

Provedor de Serviço .NET - STORK

SECURE IDENTITY ACROSS BORDERS LINKED

Pedido SAML

País do SP LOCAL
País do Cidadão LOCAL
Identificador do SP PT-SP
QAA Level 3
Emissor do SAML http://localhost/SP/
SP Return URL http://localhost/SP/

Atributos

Atributo Todos os atributos? Obrigatório? Todos Obrigatórios?

eIdentifier
givenName
surname
inheritedFamilyName
adoptedFamilyName
gender
dateOfBirth
countryCodeOfBirth
nationalityCode
maritalStatus
textResidenceAddress
canonicalResidenceAddress
eMail
title
residencePermit
pseudonym
age
isAgeOver
signedDoc
citizenQAALevel
fiscalNumber

Send

Figura 1: Página de Inicio - DemoSP:NET

Seleccione los atributos que desea solicitar en el proceso de autenticación y pulse “Send”.



Cuando un ciudadano accede al programa STORK, el proveedor de servicio hará una petición de datos del usuario, sobretodo cuando se trata de la primera vez que accede. Estos datos se extraen de sus credenciales o de bases de datos verificadas y mantenidas por las autoridades competentes, de tal manera que el proveedor de servicios pueda fiarse totalmente de los datos recibidos. Además, la calidad de estos datos está ligada al nivel de garantía de calidad de las credenciales requeridas por el proveedor de servicios; algunos de ellos pueden solicitar unos datos de calidad alta, mientras que otros se conformarán con un nivel medio o más bajo.

El proveedor de servicios se basa en los resultados obtenidos de la autenticación online para establecer la identidad de un subscriptor/usuario para realizar la transacción. El proveedor de servicios y el verificador pueden ser la misma entidad o pueden ser entidades diferentes. Si son entidades diferentes, el proveedor de servicios recibe una confirmación por parte del verificador.

El Proveedor de Servicios es responsable de validar que la confirmación vino de un verificador de confianza. Cuando estas confirmaciones indican la fecha de su creación o atributos asociados al demandante, el Proveedor de Servicios es también responsable de verificar esta información.

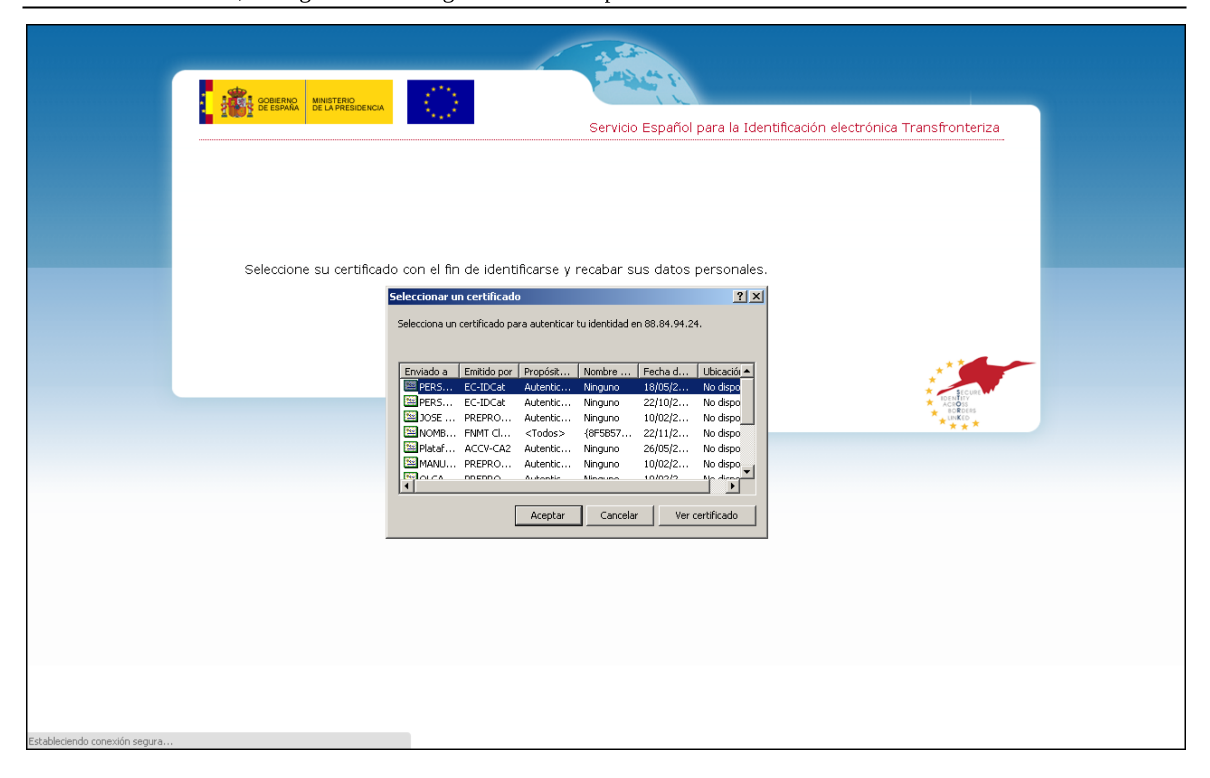
El Proveedor de Servicios determina que credenciales son requeridas para proporcionar al demandante o subscriptor acceso. Es por lo tanto el Proveedor de Servicios el que determina el nivel de autenticación para acceder a los datos.

Examinemos el siguiente ejemplo que detalla el funcionamiento del flujo de una petición:

Si un usuario desea acceder a un Proveedor de Servicios español, el usuario comienza el proceso de autenticación seleccionando “autenticarse” con el proveedor de servicios. El proveedor de servicios envía entonces una petición de autenticación y la información relativa al nivel de la QAA (Quality Authentication Assurance) requerida al PEPS español para que proceda con la verificación del demandante. El PEPS español pregunta entonces al usuario qué país le expidió la Identidad electrónica que va a utilizar para autenticarse y le proporciona un listado de Estados Miembros. El usuario selecciona uno de este listado; y el PEPS español envía la petición de autenticación al país seleccionado.

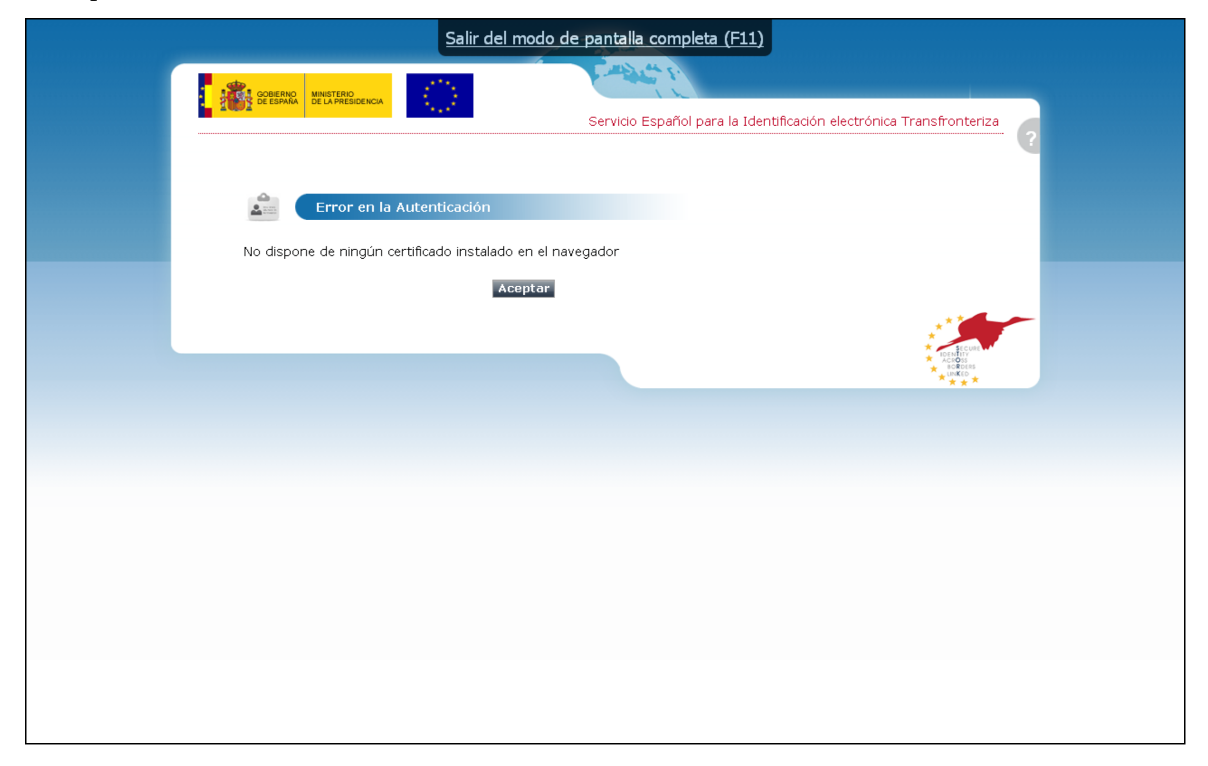
Este país proporciona al usuario un listado de Identidades electrónicas que cumplen con la autenticación demandada y con los requisitos del nivel de servicio de QAA. El usuario escoge en ese momento la Identidad electrónica con la que quiere autenticarse.





La validación de la Identidad electrónica seleccionada se lleva a cabo basándose en la interacción existente entre este país y el usuario; el país demanda a su IDP (Proveedor de Identificación) la validación de la Identidad electrónica. Se pueden dar varios casos:

- si no se puede realizar la validación, se informa al usuario y el proceso termina. El fin del proceso consiste en el envío por parte del usuario de un mensaje SAML informado del tipo de error producido.





- si se consigue validar su Identidad electrónica, el país del usuario crea una confirmación que es presentada al usuario para que de su consentimiento, paso necesario ya los datos son personales, y por lo tanto protegidos por la ley.



- si el usuario niega su consentimiento, el proceso termina (con el envío del un mensaje SAML al SP informando de la negación del consentimiento).
- si lo da, se envía al PEPS español que a su vez se pone en contacto con el proveedor de servicios que responde afirmativamente a la demanda del usuario. En este caso el SP recibe un mensaje SAML con la información solicitada sobre el ciudadano.

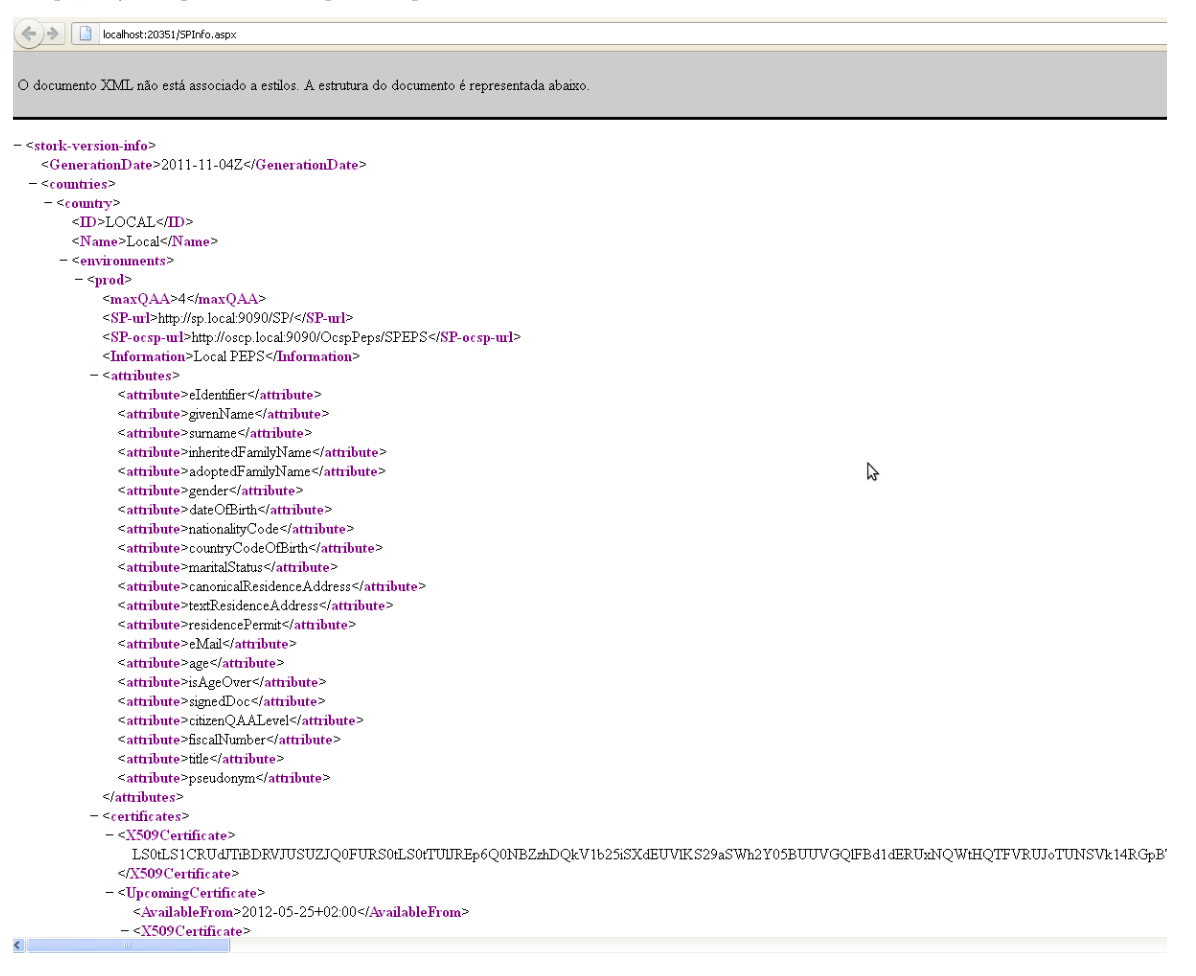
Si la autenticación termina en éxito, deberá ver una tabla con los atributos pedidos junto con el valor obtenido, como se ve en la Figura 2.



Figura 2: Página de Retorno - DemoSP .NET



El fichero de control de versiones para SPs version control file está disponible aquí: "http(s)://your.ip.addres/SP/spInfo.aspx".





6 SAML Engine API

6.1 Ejemplos de uso

6.1.1 Generando una petición de autenticación STORK

```
//Creating STORK Authentication Request --------------------------------
SAMLRequest request = new SAMLRequest();

//Filling Authentication Request fields --------------------------------
request.Destination = (…);
request.AssertionConsumerServiceURL = (…);
request.Country = (…);
request.ProviderName = (…);
request.Issuer = (…);
request.QAALevel = (…);
request.Id = (…);

//Loading Stork attributes to request
request.AddAttribute(AttributeID, isRequired);

//Getting STORKSAMLEngine object  --------------------------------------
SAMLEngine samlEngine = SAMLEngine.Instance;
samlEngine.Init(HttpContext.Current.Server.MapPath(".") + "/bin/");
XmlDocument xml = samlEngine.GenerateRequest(request);
Convert.ToBase64String(Encoding.UTF8.GetBytes(xml.OuterXml));
```

Este *SAMLRequest* debe ser colocado dentro de un formulario HTML. Por ejemplo, puede usar el método *WebUtils' PreparePOSTForm* en el método *Default.aspx.cs' do_POST*:

```
postForm = WebUtils.PreparePOSTForm(
                        samlRequestField, relayStateField, countryField,
                        TextBoxSAMLrequest.Text, "State information to be
persisted across", countryList.SelectedValue,
DropDownListCPEPSCountry.SelectedValue);
```

6.1.2 Validando y leyendo una respuesta de autenticación STORK

Primero, se recibe dentro de un HTTP POST el parámetro "SAMLResponse". Entonces:

```
//Decodes incoming SAML Response
byte[] reqDataB64 = Convert.FromBase64String(SAMLResponse);

//Generate XML Object
string reqData = Encoding.UTF8.GetString(reqDataB64);

XmlDocument xml = new XmlDocument();
xml.PreserveWhitespace = true;
xml.LoadXml(reqData);

//Create the SAML Engine instance and validate SAML response
SAMLEngine.Instance.Init(HttpContext.Current.Server.MapPath(".") + "/bin/");
SAMLResponse samlResponse = SAMLEngine.Instance.HandleResponse(xml);
```




```
//Get Attribute List
foreach (int attrId in samlResponse.GetAttributeIds()) {
   // It's a Complex Value?
   if (samlResponse.isAttributeComplex(attrId))
   {
      // Get the complex attribute's value
      Dictionary<string, string> attrValue =
samlResponse.GetAttributeComplexValue(attrId);
      // Get Attribute's friendly name:
      string attrname = CitizenAttributes.Instance.GetFriendlyName(attrId)
      // Get complex attribute's values
      foreach ( String key in attrValue.Keys)
      {
         // Get the complex attribute's value for key
         // attrValue[key]
         // E.g.:
         //       Attribute - canonicalAddress
         //       key - postalCode
         //       attrValue[key] - 28038
      }
      // Get Attribute's status:
      // samlResponse.GetAttributeStatusStr(attrId)
   }
   else
   {
      // It's a simple value!
      // Get attribute's value:
      string attrValue = samlResponse.GetAttributeValue(attrId);
      // Get attribute's status
      string attrStatus = samlResponse.GetAttributeStatusStr(attrId);
   }
}
```

7 Conjunto de certificados de prueba

Se distribuye junto con la aplicación DemoSP.NET un conjunto de de certificados para facilitar la realización de pruebas transfronterizas.

Nombre del fichero del certificado	País	Contraseña
Ana_Vzorec_02.pfx	Eslovenia	Ana_Vzorec_02
Alice Auth*.p12	Bélgica	BelgaCom.
Stork_Active.p12	Portugal	#ptcert!
sanmiguel.p12	España	1234

8 Preguntas frecuentes

Nota que hay más preguntas frecuentes en el documento “Introducción a STORK para proveedores de Servicios”

¿Para qué sirve el control de versiones?

Mediante el control de versiones la autoridad española de STORK puede conocer la versión del software que Vd tiene instalado y por lo tanto puede saber si una modificación que está planteando implantar es compatible o no con sus instalaciones. De esta forma se evitan problemas de incompatibilidades.

¿Dónde puedo acudir a soporte?

mailto:stork@indra.es



9 ANEXO: Petición de Alta como Proveedor de Servicios con acceso a la Plataforma STORK

Fecha_Petición	*Fecha actual*
Nombre	*Nombre del Proveedor de Servicio*
Descripción	
Entorno	*PRE o PRO*
Persona_Contacto	*Persona de Contacto del Proveedor de Servicio (teléfono y email)*
Cerificado_SP	*Parte pública del certificado usado por el Proveedor de Servicio en la firma SAML*
-----BEGIN CERTIFICATE----- -----END CERTIFICATE-----	
Fecha_ prevista	*Fecha de Inicio prevista para pruebas en el entorno indicado*

Nota que nombre del proveedor de servicio y el certificado de firma tienen que coincidir con los valores configurados en 4.1.1.